On Furtwängler's theorems and second case of Fermat's Last Theorem

Roland Quême

2013 Apr 23

Abstract

This article, complement to the article [Que], deals with some generalizations of Futwängler's theorems for the second case of Fermat's Last Theorem (FLT2). Let p be an odd prime, ζ a pth primitive root of unity, $K := \mathbb{Q}(\zeta)$ and $C\ell_K$ the class group of K. A prime q is said *p-principal* if the class $c\ell_K(\mathfrak{q}_K) \in C\ell_K$ of any prime ideal $\mathfrak{q}_K$ of $\mathbb{Z}_K$ over q is the pth power of a class. Assume that FLT2 fails for (p, x, y, z) where x, y, z are mutually coprime integers, p divides y and $x^p + y^p + z^p = 0$.

Let q be a prime dividing $\frac{(x^p+y^p)(y^p+z^p)(z^p+x^p)}{(x+y)(y+z)(z+x)}$ and $\mathfrak{q}_K$ be any prime ideal of K over q. We obtain the p-power residue symbols relations

$$\left(\frac{p}{\mathfrak{q}_K}\right)_K = \left(\frac{1-\zeta^j}{\mathfrak{q}_K}\right)_K \text{ for } j = 1, \ldots, p-1.$$

As an application, we prove that: if Vandiver's conjecture holds for p then q is a p-principal prime.

Similarly, let q be a prime dividing dividing $\frac{(x^p-y^p)(y^p-z^p)(z^p-x^p)}{(x-y)(y-z)(z-x)}$ and $\mathfrak{q}_K$ be the prime ideal of K over q dividing $(x\zeta - y)(z\zeta - y)(x\zeta - z)$. We give an explicit formula for the p-power residue symbols $\left(\frac{\epsilon_k}{\mathfrak{q}_K}\right)_K$ for all k with $1 < k \leq \frac{p-1}{2}$, where ϵ_k is the cyclotomic unit given by $\epsilon_k =: \zeta^{(1-k)/2} \cdot \frac{1+\zeta^k}{1+\zeta}$.

The principle of proofs rely on the p-Hilbert class field theory.

[1]

---

[1]

- *Keywords:* Fermat's Last Theorem, cyclotomic fields, cyclotomic units, class field theory, Vandiver's and Furtwängler's theorems
- *AMS subject classes :* 11D41, 11R18, 11R37

1 Introduction

1.1 General notations and definitions

- Let $p > 3$ be a prime, $\zeta := e^{\frac{2\pi i}{p}}$, $K := \mathbb{Q}(\zeta)$ the pth cyclotomic number field, $\mathbb{Z}_K$ the ring of integers of K, and $\mathfrak{p} = (1-\zeta)\mathbb{Z}_K$ the prime ideal of $\mathbb{Z}_K$ over p. Let $g := \mathrm{Gal}(K/\mathbb{Q})$, for $k \not\equiv 0 \mod p$ and $s_k : \zeta \to \zeta^k$ the $p-1$ distinct elements of g.

- Let $C\ell_K$, $C\ell$ and $C\ell^-$ be respectively the class group of K, the p-class group of K and the negative part of the p-class group of K. For any ideal $\mathfrak{a}$ of K, let us note $c\ell_K(\mathfrak{a})$, $c\ell(\mathfrak{a}), c\ell^-(\mathfrak{a})$ be respectively the class of $\mathfrak{a}$ in $C\ell_K$, $C\ell$ and $C\ell^-$.

- A prime q is said *p-principal* if the class $c\ell_K(\mathfrak{q}_K) \in C\ell_K$ of any prime ideal $\mathfrak{q}_K$ of $\mathbb{Z}_K$ above q is the pth power of a class, which is equivalent to $\mathfrak{q}_K = \mathfrak{a}^p(\alpha)$, for an ideal $\mathfrak{a}$ of K and an $\alpha \in K^\times$. This contains the case where the class $c\ell_K(\mathfrak{q}_K)$ is of order coprime with p.

- For any $\alpha \in K$ and prime ideal $\mathfrak{q}_K$ of K, we use the pth power residue symbol notation $\left(\frac{\alpha}{\mathfrak{q}_K}\right)_K$.

- We will adopt in the sequel the following notations for an hypothetic counterexample to $FLT2$. We say that $FLT2$ would fail for (p,x,y,z) if we had
$$x^p + y^p + z^p = 0,$$
with $x, y, z \in \mathbb{Z}\backslash\{0\}$ pairwise coprime and p dividing y.

1.2 Main results

Let q be a prime dividing $\frac{(x^p+y^p)(y^p+z^p)(z^p+x^p)}{(x+y)(y+z)(z+x)}$ and $\mathfrak{q}_K$ be any prime ideal of K over q. We obtain the p-power residue symbols relations (see theorem 2.4)

$$\left(\frac{p}{\mathfrak{q}_K}\right)_K = \left(\frac{1-\zeta^j}{\mathfrak{q}_K}\right)_K \text{ for } j = 1, \dots, p-1.$$

As an application, we prove that: if Vandiver's conjecture fails for p then q is a p-principal prime (see theorem 2.5).

Similarly, let q be a prime dividing dividing $\frac{(x^p-y^p)(y^p-z^p)(z^p-x^p)}{(x-y)(y-z)(z-x)}$ and $\mathfrak{q}_K$ be the prime ideal of K over q dividing $(x\zeta - y)(z\zeta - y)(x\zeta - z)$. We give an explicit formula for the p-power residue symbols $\left(\frac{\epsilon_k}{\mathfrak{q}_K}\right)_K$ for all k with $1 < k \leq \frac{p-1}{2}$, where ϵ_k is the cyclotomic unit given by $\epsilon_k =: \zeta^{(1-k)/2} \cdot \frac{1+\zeta^k}{1+\zeta}$ (see theorem 2.7).

This article is a complement to the article [GQ] dealing with *Strong Fermat's Last Theorem conjecture (SFLT)* and article [Que] dealing with *second case of Strong Fermat's Last Theorem conjecture (SFLT2)*.

2 Detailed results and proofs

We give at first a general lemma.

Lemma 2.1. *Suppose that $FLT2$ fails for (p, x, y, z) with $p|y$. If $q \neq p$ satisfies*

$$y \equiv 0 \mod q \text{ and } x + z \not\equiv 0 \mod q,$$

then $q - 1 \equiv 0 \mod p^2$.

Proof.

- From Barlow-Abel relations

$$x + z = p^{\nu p-1} y_0^p,\ \frac{x^p + z^p}{x + z} = p y_1^p,\ y = -p^\nu y_0 y_1,\ \nu \geq 1,$$

- Suppose that $q|\frac{x^p+z^p}{x+z}$ with p prime to κ and search for a contradiction: let $\mathfrak{q}_K$ be a prime ideal of $\mathbb{Z}_K$ lying over q. From $q|y$ and the Barlow-Abel relation $x + y = z_0^p$, we have

$$\left(\frac{x}{\mathfrak{q}_K}\right)_K = \left(\frac{x + y}{\mathfrak{q}_K}\right)_K = \left(\frac{z_0^p}{\mathfrak{q}_K}\right)_K = 1.$$

  Similarly $\left(\frac{z}{\mathfrak{q}_K}\right)_K = 1$, so $x^{(q-1)/p} - z^{(q-1)/p} \equiv 0 \mod \mathfrak{q}_K$. We get

$$q \mid x^{(q-1)/p} - z^{(q-1)/p} \text{ and } q \mid x^p + z^p.$$

- If we suppose $\kappa = \frac{q-1}{p}$ prime to p, we have $\kappa = \frac{q-1}{p}$ even and $x^\kappa \equiv (-z)^\kappa \mod q$ and $x^p \equiv (-z)^p \mod q$, thus $q \mid x + z$ by a Bézout relation between p and n (absurd).

□

2.1 On the primes q dividing $\frac{(x^p+y^p)(y^p+z^p)(z^p+x^p)}{(x+y)(y+z)(z+x)}$

1. We assume that $FLT2$ fails for (p, x, y, z). This section contains some general strong properties of the primes q dividing $\frac{(x^p+y^p)(y^p+z^p)(z^p+x^p)}{(x+y)(y+z)(z+x)}$ complementary to Furtwängler's theorems. Here, we don't assume that q is p-principal or not, thus this subsection brings complementary informations to corollary 2.7 of [Que].

2. Let us define the totally real cyclotomic units

$$\varpi_a =: \zeta^{(1-a)/2} \cdot \frac{1-\zeta^a}{1-\zeta},\ 1 \leq a \leq p-1,$$

where this definition implies $\varpi_1 = 1$. Recall that the cyclotomic units of K are generated by the ϖ_a for $1 < a < \frac{p}{2}$. We have $\varpi_a = -\varpi_{p-a}$: indeed we have $\varpi_a = \zeta^{(1-a)/2} \cdot \frac{1-\zeta^a}{1-\zeta}$ and $\varpi_{p-a} = \zeta^{(1-(p-a))/2} \cdot \frac{1-\zeta^{p-a}}{1-\zeta} = \zeta^{(1+a)/2} \cdot \frac{1-\zeta^{-a}}{1-\zeta} = \zeta^{1-a)/2} \cdot \frac{\zeta^a-1}{1-\zeta} = -\varpi_a$.

Lemma 2.2. *Assume that FLT2 fails for (p,x,y,z) with $p|y$. Let $\mathfrak{q}_K$ be a prime ideal of $\mathbb{Z}_K$ such that $x\zeta + y \equiv 0 \mod \mathfrak{q}_K$ (or $z\zeta + y \equiv 0 \mod \mathfrak{q}_K$). Then*

$$q \equiv 1 \mod p^2 \text{ and } \left(\frac{\zeta}{\mathfrak{q}_K}\right)_K = \left(\frac{p}{\mathfrak{q}_K}\right)_K = \left(\frac{1-\zeta}{\mathfrak{q}_K}\right)_K = 1.$$

Proof.

- Suppose that $x\zeta + y \equiv 0 \mod \mathfrak{q}_K$. We have $q|z$, so $q \equiv 1 \mod p^2$ from First Furtwängler's theorem, so $\left(\frac{\zeta}{\mathfrak{q}_K}\right)_K = 1$ and $\left(\frac{x}{\mathfrak{q}_K}\right)_K = \left(\frac{y}{\mathfrak{q}_K}\right)_K$, so $\left(\frac{x+z}{\mathfrak{q}_K}\right)_K = \left(\frac{y+z}{\mathfrak{q}_K}\right)_K$, so

$$\left(\frac{p^{\nu p-1}y_0^p}{\mathfrak{q}_K}\right)_K = \left(\frac{x_0^p}{\mathfrak{q}_K}\right)_K \text{ with } \nu \in \mathbb{N}_{\geq 1},$$

from Barlow-Abel relations, and finally $\left(\frac{p}{\mathfrak{q}_K}\right)_K = 1$. In the other hand, we have

$$x+y = z_0^p \equiv x(1-\zeta) \equiv (x+z)(1-\zeta) \equiv p^{\nu p-1}y_0^p(1-\zeta) \mod \mathfrak{q}_K,$$

so

$$\left(\frac{1-\zeta}{\mathfrak{q}_K}\right)_K = 1.$$

- Suppose that $z\zeta + y \equiv 0 \mod \mathfrak{q}_K$. The proof is similar with z in place of x.

□

Lemma 2.3. *Suppose that FLT2 fails for (p,x,y,z) with $p|y$. Let $q \neq p$ be a prime and $\mathfrak{q}_K$ be a prime ideal of $\mathbb{Z}_K$ over q. Then we have for $k = 1,\dots,p-2$:*

1. *If $\mathfrak{q}_K$ divides $x\zeta + y$ then $\left(\frac{x+\zeta^k y}{\mathfrak{q}_K}\right)_K = \left(\frac{\varpi_{k+1}}{\mathfrak{q}_K}\right)_K$.*
2. *If $\mathfrak{q}_K$ divides $z\zeta + y$ then $\left(\frac{z+\zeta^k y}{\mathfrak{q}_K}\right)_K = \left(\frac{\varpi_{k+1}}{\mathfrak{q}_K}\right)_K$.*
3. *If $\mathfrak{q}_K$ divides $x\zeta + z$ and $p \mid y$ then $\left(\frac{x+\zeta^k z}{\mathfrak{q}_K}\right)_K \left(\frac{p}{\mathfrak{q}_K}\right)_K = \left(\frac{\varpi_{k+1}}{\mathfrak{q}_K}\right)_K$.*

Proof.

1. From $x\zeta + y \equiv 0 \mod \mathfrak{q}_K$ we get

$$x + \zeta^k y \equiv x(1 - \zeta^{k+1}) \mod \mathfrak{q}_K,\ k = 1, \dots, p-2.$$

thus

$$\frac{x+\zeta^k y}{x+y} \equiv \frac{1-\zeta^{k+1}}{1-\zeta} \mod \mathfrak{q}_K,\ \text{for } k = 1, \dots, p-2.$$

In the other hand, $\varpi_{k+1} = \zeta^{(1-(k+1))/2} \cdot \frac{1-\zeta^{k+1}}{1-\zeta}$ is a totally real cyclotomic unit, so

$$\frac{x+\zeta^k y}{x+y} \equiv \varpi_{k+1}\zeta^{k/2} \mod \mathfrak{q}_K,\ \text{for } k = 1, \dots p-2,$$

so

$$\Big(\frac{x+\zeta^k y}{\mathfrak{q}_K}\Big)_K = \Big(\frac{\varpi_{k+1}}{\mathfrak{q}_K}\Big)_K \Big(\frac{\zeta^{k/2}}{\mathfrak{q}_K}\Big)_K \text{ for } k = 1, \dots, p-2,$$

because $x + y \in K^{\times p}$ and finally

$$\Big(\frac{x+\zeta^k y}{\mathfrak{q}_K}\Big)_K = \Big(\frac{\varpi_{k+1}}{\mathfrak{q}_K}\Big)_K \text{ for } k = 1, \dots, p-2,$$

because $q \equiv 1 \mod p^2$ obtained by the first Theorem of Furtwängler.

2. The proof is similar to *item 1.* with z in place of x.

3. In that case we have $x + z = p^{\nu p-1}y_0^p$ with $\nu > 0$ and so $x + z \in p^{-1}K^{\times p}$ and $p^2 | q-1$ as proved in lemma 2.1.

□

Theorem 2.4. *Assume that the second case of FLT fails for (p, x, y, z) with $p|y$. Let q be a prime dividing $\frac{x^p+y^p}{x+y}$ (or $\frac{z^p+y^p}{z+y}$ or $\frac{x^p+z^p}{x+z}$). Let $\mathfrak{q}_K$ be <u>the</u> prime ideal of $\mathbb{Z}_K$ over q dividing $x\zeta + y$ (or $z\zeta + y$ or $x\zeta + z$).*

If the p-class $c\ell(\mathfrak{q}_K) \in C\ell^-$ we have:

1. *The prime q satisfies the congruence $q \equiv 1 \mod p^2$.*

2. *$\mathfrak{q}_K$ satisfies the following power residue symbols values:*

   (a) *If $\mathfrak{q}_K | x\zeta + y$ (or $z\zeta + y$) then*

$$\Big(\frac{p}{\mathfrak{q}_K}\Big)_K = \Big(\frac{1-\zeta^j}{\mathfrak{q}_K}\Big)_K = 1 \textit{ for } j = 1, \dots, p-1.$$

(b) *If* $\mathfrak{q}_K | x\zeta + z$ *then*

$$\left(\frac{p}{\mathfrak{q}_K}\right)_K = \left(\frac{1-\zeta^j}{\mathfrak{q}_K}\right)_K \textit{ for } j = 1, \dots, p-1.$$

(c) *If Vandiver's conjecture holds for* p, *the prime* q *is* p*-principal.*

Proof.

- If $q | \frac{x^p+y^p}{x+y} \frac{x^p+y^p}{x+y}$, from Furtwangler's First theorem, we get $q \equiv 1 \mod p^2$. We derive that $\left(\frac{\zeta}{\mathfrak{q}_K}\right)_K = 1$ and from lemma 2.2 that $\left(\frac{p}{\mathfrak{q}_K}\right)_K = 1$. If $q | \frac{x^p+z^p}{x+z}$ then, $q \equiv 1 \mod p^2$ from lemma 2.1, which proves *item 1* of the statement.
- Suppose $q | \frac{x^p+y^p}{x+y}$.
  - From previous lemma 2.3, we have

    $$\left(\frac{x+\zeta^k y}{\mathfrak{q}_K}\right)_K = \left(\frac{\varpi_{k+1}}{\mathfrak{q}_K}\right)_K \text{ for } k = 1, \dots, p-2,$$

    and also, with $p-k$ in place of k,

    $$\left(\frac{x+\zeta^{p-k} y}{\mathfrak{q}_K}\right)_K = \left(\frac{\varpi_{p-k+1}}{\mathfrak{q}_K}\right)_K \text{ for } p-k = 1, \dots, p-2,$$

    so

    $$\left(\frac{\frac{x+\zeta^k y}{x+\zeta^{p-k} y}}{\mathfrak{q}_K}\right)_K = \left(\frac{\varpi_{k+1}\varpi_{p-k+1}^{-1}}{\mathfrak{q}_K}\right)_K \text{ for } p-k = 1, \dots, p-2, \tag{1}$$

  - For $2 \le k \le p-2$, we can write

    $$x + \zeta^k y = A_k B_k \alpha^p,$$

    with $\alpha \in K^{\times p}$, pseudo-units A_k, B_k verifying $A_k^{s_{-1}+1} \in K^{\times p}$ and $B_k^{s_{-1}-1} \in K^{\times p}$ where we recall that s_k is the $\mathbb{Q}$-isomorphism $s_k : \zeta \to \zeta^k$ of K. Let $\left(\frac{A_k}{\mathfrak{q}_K}\right)_K = \zeta^w$, we get

    $$\left(\frac{A_k^{s_{-1}}}{s_{-1}(\mathfrak{q}_K)}\right)_K = \left(\frac{A_k^{-1}}{s_{-1}(\mathfrak{q}_K)}\right)_K = \zeta^{-w},$$

    so

    $$\left(\frac{A_k}{s_{-1}(\mathfrak{q}_K)}\right)_K = \zeta^w,$$

and so $\left(\frac{A_k}{\mathfrak{q}_K s_{-1}(\mathfrak{q}_K)}\right)_K = \zeta^{2w}$. But $c\ell(\mathfrak{q}_K) \in C\ell^-$, so $(\mathfrak{q}_K s_{-1}(\mathfrak{q}_K))^n \mathbb{Z}_K = \beta \mathbb{Z}_K$ with $\beta \in \mathbb{Z}_K$ and a certain integer n coprime with p. Then

$$\left(\frac{A_k}{\mathfrak{q}_K^n s_{-1}(\mathfrak{q}_K)^n}\right)_K = \left(\frac{A_k}{\beta}\right)_K = 1,$$

because A_k is a p-primary pseudo-unit (for instance by application of Artin-Hasse reciprocity law), so $w = 0$ and $\left(\frac{A_k}{\mathfrak{q}_K}\right)_K = 1$.

– We get $\frac{x+\zeta^k y}{x+\zeta^{p-k} y} \in A_k^2 \times K^{\times p}$, so

$$(2) \qquad \left(\frac{x+\zeta^k y}{\mathfrak{q}_K}\right) = \left(\frac{x+\zeta^{p-k} y}{\mathfrak{q}_K}\right)_K \text{ for } \ k = 2, \dots, p-2.$$

which leads to

$$\left(\frac{\varpi_{k+1}}{\mathfrak{q}_K}\right)_K = \left(\frac{\varpi_{p-k+1}}{\mathfrak{q}_K}\right)_K \text{ for } k = 2, \dots, p-2.$$

– We have seen above that $\varpi_{k+1} = -\varpi_{p-k-1}$ so

$$\left(\frac{\varpi_{k+1}}{\mathfrak{q}_K}\right)_K = \left(\frac{\varpi_{p-k-1}}{\mathfrak{q}_K}\right)_K \text{ for } k = 2, \dots, p-2.$$

Then, gathering these relations involving the units $\varpi_{k+1}, \varpi_{p-k-1}, \varpi_{p-k+1}$, we get

$$\left(\frac{\varpi_{p-k+1}}{\mathfrak{q}_K}\right)_K = \left(\frac{\varpi_{p-k-1}}{\mathfrak{q}_K}\right)_K \text{ for } k = 2, \dots, p-2.$$

– Starting from $k = 2$ we get for $k = 2, 4, \dots, p-3$,

$$\left(\frac{\varpi_{p-1}}{\mathfrak{q}_K}\right)_K = \left(\frac{\varpi_{p-3}}{\mathfrak{q}_K}\right)_K = \dots = \left(\frac{\varpi_2}{\mathfrak{q}_K}\right)_K = 1,$$

because we get directly $\left(\frac{\varpi_{p-1}}{\mathfrak{q}_K}\right)_K = 1$ from its definition. Starting from $k = 3$ we get for $k = 3, 5, \dots, p-2$,

$$\left(\frac{\varpi_{p-2}}{\mathfrak{q}_K}\right)_K = \left(\frac{\varpi_{p-4}}{\mathfrak{q}_K}\right)_K = \dots = \left(\frac{\varpi_1}{\mathfrak{q}_K}\right)_K = 1,$$

because we get directly $\left(\frac{\varpi_1}{\mathfrak{q}_K}\right)_K = 1$ from its definition. Therefore we get

$$\left(\frac{\varpi_i}{\mathfrak{q}_K}\right)_K = 1 \text{ for } i = 1, \dots, p-1.$$

So, we get

$$\left(\frac{1-\zeta^i}{\mathfrak{q}_K}\right)_K = \left(\frac{1-\zeta}{\mathfrak{q}_K}\right)_K \text{ for } i = 1, \dots, p-1.$$

and finally we find again $\left(\frac{p}{\mathfrak{q}_K}\right)_K = \left(\frac{1-\zeta}{\mathfrak{q}_K}\right)_K$, seen in lemma 2.2.

From lemma 2.2 we have also $\left(\frac{1-\zeta}{\mathfrak{q}_K}\right)_K = 1$ if $\mathfrak{q}_K | x\zeta + y$ (or $\mathfrak{q}_K | z\zeta + y$), which proves *item 2.a* for $q | \frac{(x^p+y^p)(z^p+y^p}{(x+y)(z+y)}$.

- If Vandiver's conjecture holds for p the p-primary units corresponding to $C\ell^-$ are all generated by the $\varpi_i, \quad i = 1, \dots, \frac{p-1}{2}$. Therefore, the result $\left(\frac{\varpi_i}{\mathfrak{q}_K}\right)_K = 1$ for $i = 1, \dots, p-1$ obtained and the assumption that $c\ell(\mathfrak{q}_K) \in C\ell^-$ imply that $\mathfrak{q}_K$ is p-principal (application of the decomposition and reflection theorems in the p-Hilbert class field of K), if not it should be possible to find some integers $n_1, \dots, n_{(p-3)/2} \not\equiv 0 \mod p$, such that the p-primary unit $\varpi = \prod_{i=1}^{(p-3)/2} \varpi_i^{n_i}$ verifies $\left(\frac{\varpi}{\mathfrak{q}_K}\right)_K \neq 1$, contradiction which proves *item 2.c* for $q | \frac{(x^p+y^p)(z^p+y^p}{(x+y)(z+y)}$.

- Suppose at last that $q | \frac{x^p+z^p}{x+z}$: If $\mathfrak{q}_K | x\zeta + z$ and $p \mid y$ then

$$\left(\frac{x+\zeta^k z}{\mathfrak{q}_K}\right)_K \left(\frac{p}{\mathfrak{q}_K}\right)_K = \left(\frac{\varpi_{k+1}}{\mathfrak{q}_K}\right)_K,$$

(seen in lemma 2.3 *item 3.*) and similarly

$$\left(\frac{x+\zeta^{p-k} z}{\mathfrak{q}_K}\right)_K \left(\frac{p}{\mathfrak{q}_K}\right)_K = \left(\frac{\varpi_{p-k+1}}{\mathfrak{q}_K}\right)_K,$$

so we get again the relation (1)

$$\left(\frac{\frac{x+\zeta^k z}{x+\zeta^{p-k} z}}{\mathfrak{q}_K}\right)_K = \left(\frac{\varpi_{k+1}\varpi_{p-k+1}^{-1}}{\mathfrak{q}_K}\right)_K.$$

In the other hand $\frac{x+\zeta^k z}{x+\zeta^{p-k} z} = \zeta^k A$ where A is also a p-primary pseudo unit with $A^{s_{-1}+1} \in K^{\times p}$. Then the end of the proof is similar to the previous cases $q | \frac{(x^p+y^p)(z^p+y^p)}{(x+y)(z+y)}$ taking into account that we know that $p^2 | q-1$, so $\left(\frac{\zeta^k}{\mathfrak{q}_K}\right)_K = 1$, which proves *items 2b. and 2c.* of the statement if $q | \frac{x^p+z^p}{x+z}$.

□

Remark 1. In the case of an hypothetic solution $(x, y, z), \ p|y$ of the FLT2 equation, for the primes q with $c\ell(\mathfrak{q}_K) \in C\ell^-$ and $\mathfrak{q}_K | x\zeta + y$ (or $z\zeta + y$), the theorem 2.4 can be considered as a reciprocal statement to corollary 2.7 of [Que] in which $(u, v) = (x, y)$ or (z, y) for $x, y, z, \ p|y$ hypothetic solution of the Fermat's equation. In particular, we have proved:

Theorem 2.5. *Assume that Vandiver's conjecture holds for p and that the second case of FLT fails for (p, x, y, z). Then all the primes $q \neq p$ dividing $\frac{(x^p+y^p)(y^p+z^p)(z^p+x^p)}{(x+y)(y+z)(z+x)}$ are p-principal.*

2.2 Some properties of the primes q dividing $\frac{(x^p-y^p)(y^p-z^p)(z^p-x^p)}{(x-y)(y-z)(z-x)}$

1. We assume that the second case $FLT2$ fails for (p,x,y,z) with $p|y$. This subsection contains some general properties of decomposition of the primes q dividing $\frac{(x^p-y^p)(y^p-z^p)(z^p-x^p)}{(x-y)(y-z)(z-x)}$ in certain p-Kummer extensions. Here, we don't assume that q is p-principal or not, thus this subsection brings complementary informations to $SFLT2$ corollary 2.5 in [Que]. Note that, here, Furtwängler's theorems cannot be applied to these primes q, so we cannot assume that p^2 divides $q-1$.

2. Let us define the totally real cyclotomic units

$$\epsilon_a =: \zeta^{(1-a)/2} \cdot \frac{1+\zeta^a}{1+\zeta},\ 1 \le a \le p-1,$$

where we note that $\epsilon_1 = 1$ and that

$$\varepsilon_{p-a} = \zeta^{(1-(p-a))/2} \cdot \frac{1+\zeta^{p-a}}{1+\zeta} = \zeta^{(1+a)/2} \cdot \frac{1+\zeta^{-a}}{1+\zeta} = \zeta^{(1-a)/2}\frac{1+\zeta^a}{1+\zeta} = \varepsilon_a. \tag{3}$$

Lemma 2.6. *Suppose that $FLT2$ fails for (p,x,y,z) with $p|y$. Let $q \neq p$ be a prime and $\mathfrak{q}_K$ be a prime ideal of $\mathbb{Z}_K$ over q. Then we have for $k = 1,\dots,p-1$:*

1. *If $\mathfrak{q}_K | x\zeta - y$ then $\left(\frac{x+\zeta^k y}{\mathfrak{q}_K}\right)_K = \left(\frac{\zeta^{k/2}}{\mathfrak{q}_K}\right)_K \left(\frac{\epsilon_{k+1}}{\mathfrak{q}_K}\right)_K$.*
2. *If $\mathfrak{q}_K | z\zeta - y$ then $\left(\frac{z+\zeta^k y}{\mathfrak{q}_K}\right)_K = \left(\frac{\zeta^{k/2}}{\mathfrak{q}_K}\right)_K \left(\frac{\epsilon_{k+1}}{\mathfrak{q}_K}\right)_K$.*
3. *If $\mathfrak{q}_K | x\zeta - z$ then $\left(\frac{x+\zeta^k z}{\mathfrak{q}_K}\right)_K \left(\frac{p}{\mathfrak{q}_K}\right)_K = \left(\frac{\zeta^{k/2}}{\mathfrak{q}_K}\right)_K \left(\frac{\epsilon_{k+1}}{\mathfrak{q}_K}\right)_K$.*

Proof.

1. From $x\zeta - y \equiv 0 \mod \mathfrak{q}_K$ we get

$$x + \zeta^k y \equiv x(1+\zeta^{k+1}) \mod \mathfrak{q}_K,\ k = 1,\dots,p-1.$$

thus

$$\frac{x+\zeta^k y}{x+y} \equiv \frac{1+\zeta^{k+1}}{1+\zeta} \mod \mathfrak{q}_K,\ \text{for } k = 1,\dots,p-1.$$

In the other hand, for $1 \le k \le p-2$ then $\epsilon_{k+1} = \zeta^{(1-(k+1))/2} \cdot \frac{1+\zeta^{k+1}}{1+\zeta}$ is a totally real cyclotomic unit, so $\frac{x+\zeta^k y}{x+y} \equiv \epsilon_{k+1}\zeta^{k/2} \mod \mathfrak{q}_K,\ k = 1,\dots p-1$, and finally

$$\left(\frac{x+\zeta^k y}{\mathfrak{q}_K}\right)_K = \left(\frac{\zeta^{k/2}}{\mathfrak{q}_K}\right)_K \left(\frac{\epsilon_{k+1}}{\mathfrak{q}_K}\right)_K \text{ for } k = 1,\dots,p-2,$$

because $x+y \in K^{\times p}$. [2]

[2] We don't know here if $p^2|q-1$.

2. The proof is similar with z in place of x.

3. In that case we have $x+z=p^{\nu p-1}y_0^p$ with $\nu>0$ and so $x+z\in p^{-1}K^{\times p}$.

$\square$

Theorem 2.7. *Suppose that the second case of FLT fails for (p,x,y,z) with $p|y$. Let q be a prime dividing $\frac{x^p-y^p}{x-y}$ (or $\frac{y^p-z^p}{y-z}$). Let $\mathfrak{q}_K$ be the prime ideal of $\mathbb{Z}_K$ over q dividing $x\zeta-y$ (or $z\zeta-y$). Assume that the p-class $c\ell(\mathfrak{q}_K)\in C\ell^-$.* [3]

1. *If $p^2\not| \, q-1$ then q is non p-principal and satisfies*

$$\Big(\frac{\epsilon_{p-2k'-1}}{\mathfrak{q}_K}\Big)_K=\Big(\frac{\zeta^{-k'(k'+1)}}{\mathfrak{q}_K}\Big)_K \textit{ for } 1\leq k'\leq\frac{p-3}{2},$$

and

$$\Big(\frac{\epsilon_{p-2k'}}{\mathfrak{q}_K}\Big)_K=\Big(\frac{\zeta^{\frac{1}{4}-k'^2}}{\mathfrak{q}_K}\Big)_K \textit{ for } 1\leq k'\leq\frac{p-3}{2}.$$

2. *If $p^2|\,q-1$ then q satisfies*

$$\Big(\frac{1+\zeta^j}{\mathfrak{q}_K}\Big)_K=1 \textit{ for } j=1,\dots p-1.$$

Proof.

1. Let us suppose at first that $p^2\not| \, q-1$: we know that q is non p-principal, if not it should imply $p^2|q-1$ from corollary 2.5 in [Que].

   (a) From previous lemma 2.6, we have

   $$\Big(\frac{x+\zeta^k y}{\mathfrak{q}_K}\Big)_K=\Big(\frac{\zeta^{k/2}}{\mathfrak{q}_K}\Big)_K\Big(\frac{\epsilon_{k+1}}{\mathfrak{q}_K}\Big)_K \text{ for } k=1,\dots,p-2, \tag{4}$$

   and so, with $p-k$ in place of k,

   $$\Big(\frac{x+\zeta^{p-k} y}{\mathfrak{q}_K}\Big)_K=\Big(\frac{\zeta^{(p-k)/2}}{\mathfrak{q}_K}\Big)_K\Big(\frac{\epsilon_{p-k+1}}{\mathfrak{q}_K}\Big)_K \text{ for } p-k=1,\dots,p-2. \tag{5}$$

   (b) With the same proof as in thm 2.4, we get

   $$\Big(\frac{x+\zeta^k y}{\mathfrak{q}_K}\Big)=\Big(\frac{x+\zeta^{p-k} y}{\mathfrak{q}_K}\Big)_K \text{ for } \ k=2,\dots,p-2, \tag{6}$$

   which leads from (4) and (5) to

   $$\Big(\frac{\epsilon_{p-k+1}}{\mathfrak{q}_K}\Big)_K=\Big(\frac{\zeta^k}{\mathfrak{q}_K}\Big)_K\Big(\frac{\epsilon_{k+1}}{\mathfrak{q}_K}\Big)_K \text{ for } k=2,\dots,p-2. \tag{7}$$

[3] As soon as Vandiver's conjecture is true for p, this assumption is verified.

(c) In the other hand, from (3) we have

(8) $$\epsilon_{p-k-1} = \epsilon_{k+1} :$$

From (7) and (8) we derive that

(9) $$\left(\frac{\epsilon_{p-k-1}}{\mathfrak{q}_K}\right)_K = \left(\frac{\zeta^{-k}}{\mathfrak{q}_K}\right)_K \left(\frac{\epsilon_{p-k+1}}{\mathfrak{q}_K}\right)_K \text{ for k=2,...,p-2.}$$

(d) We get for the even values $k = 2k'$

$$\left(\frac{\epsilon_{p-2k'-1}}{\mathfrak{q}_K}\right)_K = \left(\frac{\zeta^{-2k'}}{\mathfrak{q}_K}\right)_K \left(\frac{\epsilon_{p-2k'+1}}{\mathfrak{q}_K}\right)_K \text{ for } 1 \leq k' \leq \frac{p-3}{2}.$$

Observing that $\epsilon_{p-1} = 1$, so $\left(\frac{\epsilon_{p-1}}{\mathfrak{q}_K}\right)_K = 1$ we get inductively

$$\left(\frac{\epsilon_{p-2k'-1}}{\mathfrak{q}_K}\right)_K = \left(\frac{\zeta^{-\sum_{j=1}^{k'} 2j}}{\mathfrak{q}_K}\right)_K \left(\frac{\epsilon_{p-1}}{\mathfrak{q}_K}\right)_K \text{ for } k' = 1, 2, \dots, \frac{p-3}{2},$$

so

$$\left(\frac{\epsilon_{p-2k'-1}}{\mathfrak{q}_K}\right)_K = \left(\frac{\zeta^{-k'(k'+1)}}{\mathfrak{q}_K}\right)_K \text{ for } 0 \leq k' \leq \frac{p-3}{2}.$$

(e) We get for the odd values $k = 2k' + 1$

$$\left(\frac{\epsilon_{p-(2k'+1)-1)}}{\mathfrak{q}_K}\right)_K = \left(\frac{\zeta^{-(2k'+1)}}{\mathfrak{q}_K}\right)_K \left(\frac{\epsilon_{p-(2k'+1)+1}}{\mathfrak{q}_K}\right)_K \text{ for } k' = \frac{p-3}{2}, \frac{p-5}{2} \dots, 1,$$

so

$$\left(\frac{\epsilon_{p-2k'}}{\mathfrak{q}_K}\right)_K = \left(\frac{\zeta^{2k'+1}}{\mathfrak{q}_K}\right)_K \left(\frac{\epsilon_{p-2k'-2}}{\mathfrak{q}_K}\right)_K \text{ for } k' = \frac{p-3}{2}, \frac{p-5}{2} \dots, 1.$$

Observing that $\epsilon_1 = 1$, so $\left(\frac{\epsilon_1}{\mathfrak{q}_K}\right)_K = 1$ we get for $k' = \frac{p-3}{2}$, so $2k' + 1 = p - 2$,

$$\left(\frac{\epsilon_3}{\mathfrak{q}_K}\right)_K = \left(\frac{\zeta^{-2}}{\mathfrak{q}_K}\right)_K \left(\frac{\epsilon_1}{\mathfrak{q}_K}\right)_K,$$

and for $k' = \frac{p-5}{2}$

$$\left(\frac{\epsilon_5}{\mathfrak{q}_K}\right)_K = \left(\frac{\zeta^{-4}}{\mathfrak{q}_K}\right)_K \left(\frac{\epsilon_3}{\mathfrak{q}_K}\right)_K,$$

and so on.

(f) Let us define $k'' := \frac{p-1}{2} - k'$, we get

$$2k'+1 = p-2k'', \text{ for } k' = \frac{p-3}{2}, \ldots, 1 \text{ corresponding to } \; k'' = 1, \ldots, \frac{p-3}{2}.$$

It follows that

$$\left(\frac{\epsilon_{p-2k'}}{\mathfrak{q}_K}\right)_K = \left(\frac{\zeta^{\sum_{j=1}^{k''} -2j}}{\mathfrak{q}_K}\right)_K \left(\frac{\epsilon_1}{\mathfrak{q}_K}\right)_K \text{ for } k' = \frac{p-3}{2}, \frac{p-5}{2}, \ldots, 1,$$

so

$$\left(\frac{\epsilon_{p-2k'}}{\mathfrak{q}_K}\right)_K = \left(\frac{\zeta^{-k''(k''+1)}}{\mathfrak{q}_K}\right)_K \text{ for } 1 \leq k' \leq \frac{p-3}{2},$$

so

$$\left(\frac{\epsilon_{p-2k'}}{\mathfrak{q}_K}\right)_K = \left(\frac{\zeta^{-(\frac{p-1}{2}-k')(\frac{p-1}{2}-k'+1)}}{\mathfrak{q}_K}\right)_K \text{ for } 1 \leq k' \leq \frac{p-3}{2},$$

and finally

$$\left(\frac{\epsilon_{p-2k'}}{\mathfrak{q}_K}\right)_K = \left(\frac{\zeta^{\frac{1}{4}-k'^2}}{\mathfrak{q}_K}\right)_K \text{ for } 1 \leq k' \leq \frac{p-3}{2}.$$

2. Let us suppose that $q \equiv 1 \mod p^2$: then $\left(\frac{\zeta}{\mathfrak{q}_K}\right)_K = 1$ and from relation (9) we get

$$\left(\frac{\epsilon_{p-k-1}}{\mathfrak{q}_K}\right)_K = \left(\frac{\epsilon_{p-k+1}}{\mathfrak{q}_K}\right)_K \text{ for } k = 2, \ldots, p-2.$$

In the other hand we have $\left(\frac{\epsilon_{p-1}}{\mathfrak{q}_K}\right)_K = \left(\frac{\epsilon_1}{\mathfrak{q}_K}\right)_K = 1$ and so

$$\left(\frac{\epsilon_j}{\mathfrak{q}_K}\right)_K = 1 \text{ for } j = 1, \ldots, p-1.$$

A straightforward computation shows that $\left(\frac{\epsilon_1 \ldots \epsilon_{p-1}}{\mathfrak{q}_K}\right)_K = \left(\frac{1+\zeta}{\mathfrak{q}_K}\right)_K$ and we derive that

$$\left(\frac{1+\zeta}{\mathfrak{q}_K}\right)_K = 1,$$

and finally that

$$\left(\frac{1+\zeta^j}{\mathfrak{q}_K}\right)_K = 1 \text{ for } j = 1, \ldots, p-1.$$

which achieves the proof for $p^2 | q-1$.

$\square$

Acknowledgments: I would like to thank Georges Gras for pointing out many errors in the preliminary versions and for suggesting many improvements to me for the content and form of the article.

References

[Fur] P. Furtwängler, *Letzter Fermatschen Satz und Eisensteins'ches Reciprozitätsgesetz*, Sitzungsber, Akad. d. Wiss. Wien., Abt. IIa, 121, 1912, 589–592.

[Gr1] G. Gras, *Class Field Theory, From Theory to Practice*, Springer, 2003.

[Gr2] G. Gras, *Analysis of the classical cyclotomic approach of Fermat's Last Theorem*, Publications Mathématiques de Besançon, 2010.

[GQ] G. Gras and R. Quême, *Vandiver papers on cyclotomy revisited and Fermat's Last Theorem*, Publications Mathématiques de Besançon (2012/2), 47-111.

[Que] R. Quême, *On second case of Strong Fermat's Last Theorem conjecture*, preprint submitted arXiv.

[Rib1] P. Ribenboim, *13 Lectures on Fermat's Last Theorem*, Springer-Verlag, 1979. *Introduction to cyclotomic fields, second edition*, Springer, 1997.

Roland Quême
13 avenue du château d'eau
31490 Brax
France
mailto: roland.queme@gmail.com